UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/973,447	10/09/2001	Edward R. Rowe	07844-448001	7875

21876 7590 01/11/2006

FISH & RICHARDSON P.C.
P.O. Box 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 01/11/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/973,447	ROWE, EDWARD R.	
	Examiner	Art Unit	
	Jung W. Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 November 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17,23-29 and 32-37* is/are rejected.

7)☒ Claim(s) *18-22,30,31 and 38* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 February 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This Office action is in response to the amendment filed on November 18, 2005.

2. Claims 1-38 are pending.

3. Claims 1, 2, 26, 32 and 34-36 are amended.

4. Claims 37 and 38 are new.

5. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Response to Amendment

6. The objections to the drawings are withdrawn. Formal drawings were submitted on February 5, 2002.

7. The objections to claims 32 and 36 are withdrawn as the amendment overcomes the objections.

8. The 112/1st paragraph rejection to claim 2 is withdrawn as the amendment overcomes the rejection.

9. The 112/2nd paragraph rejection to claim 1 is withdrawn as the amendment overcomes the rejection.

10. The 101 rejection to claims 1-36 are withdrawn as the amendments to the claims overcome the 101 rejections.

Response to Arguments

11. Applicant's arguments, see pg. 11-12, filed November 18, 2005, with respect to the rejection(s) of claim(s) 1-36 under Takeda '189 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Peinado et al USPN 6,772,340.

Claim Rejections - 35 USC § 112

12. Claim 37 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 37 recites the limitation "the set of permission rights" in line 1. There is insufficient antecedent basis for this limitation in the claim.

13. Claim 25 is rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential structural cooperative relationships of elements, such omission amounting to a gap between the necessary structural connections. See MPEP § 2172.01. Claim 25 defines the limitation, inter alia, wherein providing the first key in an access controlled manner comprises sending information used to synthesize the first key in a rights management file and wherein the rights management file enables access to the private key. However, the specification discloses that the feature "wherein the rights management file enables access to the private key" is enabled when

public key encryption is used and the permission rights for adding skeleton keys to documents data structures or files are given (specification, pg. 7, 1st full paragraph, 8th sentence). Parent claim 24 defines the use of public key encryption; however, the structural element of the permission rights for adding skeleton keys to documents data structures or files being given is not defined in claim 25.

Claim Rejections - 35 USC § 102

14. Claims 1, 3, 8-11, 13-16, 23, 34 and 37 are rejected under 35 U.S.C. 102(e) as being anticipated by Peinado et al. USPN 6,772,340 (hereinafter Peinado).

15. As per claim 1, Peinado discloses a computer-implemented method for managing access to electronic documents, comprising:

a. associating a first key with an encrypted document decryption key, the encrypted document decryption key being associated with an encrypted document, the encrypted document decryption key when decrypted yielding a document decryption key usable to decrypt the encrypted document, the first key being usable to decrypt the encrypted document decryption key; and providing the first key in an access controlled manner to users for use in opening the encrypted document (fig. 5a, reference nos. 513, 515 and 517; fig. 5b, reference nos. 519, 521 and 523; col. 16:6-14; 17:12-30; 17:49-18:8; 23:58-24:10).

16. As per claim 3, Peinado discloses the method further comprising:

b. encrypting the first key and associating with the encrypted first key a second key that can be used to decrypt the encrypted first key (col. 23:6-24); and

c. providing the second key in an access controlled manner to users for use in opening all documents that can be opened through use of the first key (fig. 5a, reference no 517 and fig. 5b, reference nos. 519, 521 and 523).

17. As per claim 8, Peinado further discloses the step of providing the first key in an access controlled manner comprises sending the first key to users in rights management information specific to systems of the users to whom the first key is sent (col. 18:9-25).

18. As per claim 9, Peinado further discloses the rights management information comprises a rights management file (col. 24:53-67).

19. As per claim 10, Peinado further discloses the step of providing the first key in an access controlled manner comprises sending information used to synthesize the first key in rights management information (col. 21:11-62).

20. As per claim 11, Peinado discloses the method further comprising storing the encrypted first key in rights management file information for the first key (col. 24:53-67).

21. As per claim 13, Peinado discloses the method further comprising providing a document decryption key in an access controlled manner to users for accessing the document without using the first key (col. 15:53-16:4).

22. As per claim 14, Peinado discloses the method further comprising associating a unique identifier with the first key (fig. 3 and 8; content id and key id).

23. As per claim 15, Peinado further discloses the unique identifier is stored in the document in association with the encrypted document decryption key to associate the first key with the encrypted document decryption key (fig. 3).

24. As per claim 16, Peinado further discloses the rights management information provides a license and defines a set of permission rights associated with the license (col. 24:53-67).

25. As per claim 23, Peinado discloses the encrypted document decryption key is encrypted by an encryption key that is different from the first key (col. 16:6-14).

26. As per claim 34, it is a claim corresponding to claim 1 and it does not teach or define above the information claimed in claim 1. Therefore, claim 34 is rejected as being anticipated by Peinado for the same reasons set forth in the rejection of claim 1.

27. As per claim 37, Peinado further discloses a set of permission rights specifies a right allowing a holder of the first key to add to a second encrypted document a second encrypted document decryption key that can be decrypted by the first key and, when decrypted by the first key, yielding a second document decryption key that is usable to decrypt the encrypted document (figs. 3 and 8, each content is associated with a decryption key that is encrypted using the public key of the black box).

Claim Rejections - 35 USC § 103

28. Claim 2 is rejected under 35 USC 103(a) as being unpatentable over Peinado in view of Takeda '189 USPN 6,336,189 (hereinafter Takeda '189).

29. As per claim 2, the rejection of claim 1 under 35 USC 102(e) is incorporated herein. (supra) Peinado does not disclose storing the encrypted document key in the encrypted document. Takeda '189 discloses encrypting a decryption key, the decryption key being used to decrypt a program, wherein the encrypted decryption key is appended to a partially encrypted program (col. 8:36-50). This enables instant access to the decryption key to unwrap the program. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to store the encrypted document key in the encrypted document. One would be motivated to do so to facilitate access to the decryption key and to form a clear association between the key and the encrypted document (Takeda '189, ibid). The aforementioned cover the limitations of claim 2.

30. Claims 4-7, 17, 32, 33 and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Peinado in view of Richards USPN 6,069,957 (hereinafter Richards '957).

31. As per claims 4-7, the rejection of claim 3 under 35 U.S.C. 102(e) is incorporated herein. (supra) Peinado does not disclose a first key that decrypts multiple encrypted document decryption keys, or multiple document decryption keys that decrypts an encrypted document. Richards '957 discloses restricting access to programs whereby program material is encrypted using a key hierarchy, or "key-upon-key" encryption, whereby one key unlocks another and the last key unlocked decrypts the encrypted program (col. 1:25-30). In this scheme, more than one data decryption key is used for a given program, a different data decryption key is used for each distinct program and the data decryption keys are updated (8:36-48). It would be obvious to one of ordinary skill in the art at the time the invention was made to combine the "key-upon-key" encryption technique with the Digital Rights Management invention of Peinado since it decouples the step of securing the data-decrypting key and the user's private key, and facilitates restricted access by maintaining secure and updated key values (Richards '957, 10:5-12). Hence, the method further comprises:

d. providing a second encrypted document decryption key for a second encrypted document, the second encrypted document decryption key when decrypted yielding a document decryption key usable to decrypt the second

document, the second encrypted document decryption key being encrypted so that the first key is usable to decrypt the second encrypted document decryption key, and associating the first key with the second encrypted document decryption key (Richards '957, 8:36-48; 9:12-10:63; 'SK' is encrypted by either 'PK' or customer_code);

e. providing a third encrypted document decryption key for the second encrypted document, the third encrypted document decryption key when decrypted yielding a document decryption key usable to decrypt the second document, the third encrypted document decryption key being encrypted so that a third key is usable to decrypt the third encrypted document decryption key, associating the third key with the third encrypted document decryption key, and providing the third key in an access controlled manner to users for use in opening the second document (Richards '957, 8:44);

f. associating a third key with a second encrypted document decryption key for a second document, the second encrypted document decryption key when decrypted yielding a document decryption key usable to decrypt the second document, the second encrypted document decryption key being encrypted so that the third key is usable to decrypt the second encrypted document decryption key; encrypting the third key, associating the second key with the encrypted third key, the second key being usable to decrypt the encrypted third key, and providing the second key in an access controlled manner to users for use in

opening all documents that can be opened through use of the third key (Richards '957, 8:44; 9:12-10:63).

32. The aforementioned cover the limitations of claims 4-7.

33. As per claim 17, the rejection of claim 16 under 35 U.S.C. 102(e) is incorporated herein. (supra) Peinado does not expressly disclose the set of permission rights specifies a right allowing another key to be associated with the rights management information so that a holder of such a key has access to the first key. Richards '957 discloses restricting access to programs whereby program material is encrypted using a key hierarchy, or "key-upon-key" encryption, whereby one key unlocks another and the last key unlocked decrypts the encrypted program (col. 1:25-30). In this scheme, more than one data decryption key is used for a given program, a different data decryption key is used for each distinct program and the data decryption keys are updated (8:36-48). It would be obvious to one of ordinary skill in the art at the time the invention was made to combine the "key-upon-key" encryption technique with the Digital Rights Management invention of Peinado since it decouples the step of securing the data-decrypting key and the user's private key, and facilitates restricted access by maintaining secure and updated key values (Richards '957, 10:5-12). The aforementioned cover the limitations of claim 17.

34. As per claims 32, 33 and 36, the rejections of claims 4-7 under 35 U.S.C. 103(a) are incorporated herein. (supra) In addition, a single skeleton key can be used to open

multiple encrypted documents, a single encrypted document can be opened using more than one skeleton key, and a single skeleton key can be opened using one or more other skeleton keys (Richards '957, col. 7:24-33; 8:44-64; 9:12-18). The aforementioned cover the limitations of claims 32, 33 and 36.

35. Claims 12, 24, 26-29 and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Peinado, and further in view of Stallings, Cryptography and Network Security, Section 6.1 "Principles of Public-Key Cryptosystems" and Section 12.1 "Pretty Good Privacy" (hereinafter Stallings).

36. As per claim 12, the rejection of claim 11 under 35 U.S.C. 102(e) is incorporated herein. (supra) Peinado does not expressly disclose associating a unique identifier with the second key and storing the unique identifier in the rights management information with the encrypted first key. Stallings discloses an overview of PGP security, which includes a key management scheme, wherein a key ID is assigned to a key-decrypting key for the purpose of efficiently identifying a key that decrypts an encrypted data decryption key (pg. 365, figure 12.3 and related text). Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made to utilize key identifiers for the purpose of associating key-decrypting keys to an encrypted data-decrypting key, since it is desirous to efficiently associate such decryption keys with their encrypted values (Stallings, pg. 364, 1st paragraph). The aforementioned cover the limitations of claim 12.

37. As per claim 24, the rejection of claim 23 under 35 USC 102(e) is incorporated herein. (supra) Peinado does not disclose that the encryption key is a private key or that the first key is a public key. However, it is well known in public key encryption that the encryption key of a data value-in this case the document decryption key-can be either the public key or private key. For example, Stallings discloses that in RSA, either of the two keys can be used as the encryption key with the other being used as the decryption key (pg. 165, 2nd bullet). The primary deciding factor to determine which is used for encryption is contingent on the desire to ensure the origin of an encrypted document or to ensure the receiver of the encrypted document. In the case of Peinado, private key encryption of the document decryption key would ensure that the encrypted digital content comes from a specific trusted source. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention Peinado so that the encryption key is a private key and the first key is a public key. One would be motivated to so to ensure the origin of the encrypted decryption key and thus ensure the origin of the encrypted document as known to one of ordinary skill in the art. The aforementioned cover the limitations of claim 24.

38. As per claim 26, Peinado discloses a computer-implemented method for accessing an electronic document comprising:

g. obtaining an encrypted electronic document (col. 24:41-26:8; especially 25:3-9);

h. obtaining a collection of keys, the keys including keys that are encrypted, the keys having associations between certain pairs of them, where each association of a pair consisting of a first key and an encrypted second key indicates that the first key can be used to decrypt and thereby make usable the second key, where each association of a pair consisting of an encrypted document decryption key and the encrypted document indicates that the encrypted document decryption key, when decrypted, can be used to decrypt the encrypted document, and where a user has access to and can use certain ones of the keys in the collection (col. 23:6-24);

39. Peinado does not expressly disclose explicitly defining the associations. Stallings discloses an overview of PGP wherein one of the salient features of the invention defines an association between an encrypted data decryption key and a key-decrypting key, and between the encrypted data-decrypting key and the encrypted document, to efficiently identify which keys are sufficient to decrypt the encrypted document (pg. 365, figure 12.3). Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made to define the key pair associations and the key/document associations and use the associations to identify at least one key in the collection that is usable, directly or indirectly, to open the encrypted document, and to which the user has access for a more efficient means of identifying which keys decrypt which document (Stallings, pg. 363, last paragraph-pg. 364, first paragraph). The aforementioned cover the limitations of claim 26.

40. As per claims 27 and 28, the rejection of claim 26 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the association of the key-decrypting key decrypting the encrypted data-decrypting key, which decrypts encrypted data defines a directed path, wherein decryption of the encrypted data requires the traversal of a path from a key-decrypting key to the encrypted data. Hence, claims 27 and 28 are covered by the teachings of Peinado and Stallings.

41. As per claim 29, the rejection of claims 27 and 28 under 35 U.S.C. 103(a) are incorporated herein. (supra) In addition, each encrypted key is identified by two Ids, including a first ID corresponding to the encrypted key and a second ID corresponding to another of the keys capable of decrypting the encrypted key (Stallings, pg. 365, fig. 12.3: key ID of KUb identifies the key capable of decrypting the encrypted data-decrypting key, and the signature uniquely identifies the encrypted key and the encrypted message).

42. As per claim 35, it is a claim corresponding to claim 26 and it does not teach or define above the information claimed in claim 26. Therefore, claim 35 is rejected as being unpatentable over Peinado in view of Stallings for the same reasons set forth in the rejection of claim 26.

Allowable Subject Matter

43. Claims 18-22, 30, 31 and 38 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

44. Claim 25 would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132

January 5, 2006

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100